Data Integrity in spYdaq systems

Introduction

It many applications, especially when used for monitoring storage conditions of drugs, pharmaceuticals and blood products, it is essential that the data are a true and faithful record of the actual conditions the sensitive items have been exposed to.

To comply with certain high integrity requirements and to be validatable as part of a compliance regime such as 21 FDA CFR part 11. Stored data have to comply with certain fundamental requirements such as.

- Data are stored in secure form, not alterable by normal means.
- Calibration intervals are monitored and flagged and recorded
- Records viewed through software, are stored in encrypted form.
- Historical data retained for inspection and review online or via the PC
- Use of authority checks to ensure that only authorized individuals can use the system

Signatrol's spYdaq wireless data logging system can be used as part of an FDA21 CFR Part 11 validatable system.
To support the various facets of FDA CFR part 11 it is essential to use the system as part of an overall operating procedure that is approved by FDA.

Data Storage

Data are stored within the database in an encrypted form which is only accessible with the correct user names and password. The data cannot be altered or manipulated even if the user is an authorised used with the correct login details.

Access is controlled by a series of passwords using an Administrator/Users hierarchy.

Controlling Access

The spYdaq system uses an Administrator/User model. The Administrator has access to the system via a admin name and Password. The Administrator Name is allocated by and can only be changed by Signatrol Ltd. The administrator password can be changed by the Administrator and it is recommended that this is done at regular intervals and this should be defined in the company's procedures. Should the Administrator change then the company must contact Signatrol Ltd and request a change of administrator. The Administrator has access all programmable system parameters and can enter and disable users (Users cannot be removed for historical tracking

reasons but their access to the system can be blocked). Users can examine the system but cannot change any system parameters.

The Administrator enters Users onto the system by allocating a Username and Password. These codes are unique to a user and provide him with his electronic identity. Only the Administrator can change these login details and it is recommended that this is done at regular intervals and this should be defined in the company's procedures.

Some system parameters are configured in the base-station using a dedicated configuration disk. This disk should be controlled by the administrator and it is recommended that it is stored in a secure location. Access to the software is password controlled.

The company's procedures should include appropriate checks to ensure that the Administrator is a suitable person to be in control of the system.

Calibration Interval Calibration Interval
Any data is meaningless unless it is accurate and gives a faithful record of the conditions being monitored. For this reason it is essential to perform regulator calibration check to ensure their accuracy.

Calibration status is monitored by the system. The re-calibration interval is the period between logger calibrations. This can be set within the spYconfig software by the Administrator as 6, 12, 24, 36 Months or disabled. Recommended calibration interval is 12 months. If the period since the last calibration is within 1 month of the set period, a warning message is displayed at each against the appropriate transmitter. If the period exceeds the set period an 'Over due' message is displayed. It is important that the calibration status monitored to ensure that readings are correct and valid.

A re-calibration service is offered by Signatrol.

Validation
The FDA does not approve or endorse any products but they do validate the customer's entire control and monitoring systems. Therefore there is no such thing as an FDA validated or approved logger, however, as the customer must have his system validated it is essential that the logger complies with the regulations in all respects for the application.